Юридические исследования
Правильная ссылка на статью:
Туршин А.И. Осмотр электронных доказательств в уголовном процессе: судебный аспект // Юридические исследования. 2025. № 8. DOI: 10.25136/2409-7136.2025.8.75591 EDN: QMKBZL URL: https://nbpublish.com/library_read_article.php?id=75591

Осмотр электронных доказательств в уголовном процессе: судебный аспект

Туршин Андрей Иванович

ORCID: 0009-0005-2926-9091

аспирант; кафедра уголовно-процессуального права им. Н.В. Радутной; Российский государственный университет правосудия

152850, Россия, Ярославская область, г. Пошехонье, наб. реки Согожи, 2, кв. 9

antursh@yandex.ru

Статья из рубрики "Уголовный закон и правопорядок "

DOI:

10.25136/2409-7136.2025.8.75591

EDN:

QMKBZL

Дата направления статьи в редакцию:

15-08-2025

Дата публикации:

22-08-2025

Аннотация: Предметом исследования является осмотр электронных доказательств как следственное действие, проводимое на досудебных и судебных стадиях уголовного судопроизводства. Целью исследования является выработка научно-практических рекомендаций по вопросам осмотра электронных доказательств в ходе судебного следствия. Развитие и повсеместное распространение цифровых технологий приводит к тому, что всё чаще следы преступления оказываются зафиксированы в электронной форме. В связи с этим в доктрине появляются предложения о закреплении в УПК РФ электронных следственных действий. Отдельные особенности взаимодействия с электронной информацией получают отражение и в зарубежных странах. Однако исследователи крайне редко обращаются к стадии судебного разбирательства, не анализируя порядок исследования электронных доказательств в суде. В связи с чем в

настоящей статье предпринята попытка раскрыть особенности осмотра электронных доказательств. Для достижения поставленной цели использовались как общенаучные методы познания, так и специально-юридические методы. Метод анализа судебной практики использован для уяснения особенностей исследования электронных доказательств. Метод сравнительного правоведения позволил проанализировать релевантное законодательство зарубежных стран, установить его преимущества и недостатки. Формально-юридический метод использовался для уяснения содержания правовых норм. На основании анализа работ С.В. Зуева, Р.И. Оконенко, М.С. Сергеева, А.Б. Смушкина, К.Ю. Яковлевой установлено, что вопросы осмотра электронных доказательств судом ранее не получали широкого освещения. В результате исследования автором был проведён детальный анализ института осмотра электронных доказательств как следственного действия. Элементами новизны обладает выделение трёх основных видов осмотра электронной информации в судебном разбирательстве: осмотр сформированных на досудебном этапе электронных доказательств, осмотр электронных носителей информации, предоставленных сторонами в ходе судебного разбирательства, осмотр онлайн-источников. Вклад автора заключается в том, что была обоснована необходимость дополнения действующего уголовно-процессуального закона статьёй, регулирующей порядок судебного осмотра электронных доказательств и их приобщения к уголовному делу. Предложен проект статьи УПК РФ, посвящённой судебному осмотру электронных доказательств. Такое решение позволит устранить существующий пробел в законодательстве, предусмотрев специальное следственное действие для исследования электронных доказательств, обеспечивающее единообразие судебной практики.

Ключевые слова:

электронные доказательства, осмотр электронных доказательств, электронный осмотр, дистанционный осмотр, судебное следствие, цифровизация, следственные действия, электронные носители информации, доказывание, уголовное судопроизводство

В современном уголовном судопроизводстве часто возникает необходимость обращения к различной электронной информации, имеющей доказательственное значение. Примером являются аудио- или видеозаписи, сведения с сайтов и страниц в сети «Интернет», переписка в социальных сетях, мессенджерах, лог-файлы, метаданные и иные данные, при помощи которых устанавливаются обстоятельства, подлежащие доказыванию [17, С. 23-33].

Как известно, доказательства собираются и исследуются в строгом соответствии с установленной законом процессуальной формой — при помощи следственных и иных процессуальных действий (ст. 86, 240 УПК РФ). В ряде научных публикаций выделяются особенности электронной информации, которые определяют порядок её собирания и исследования. Так, А. Б. Смушкин пишет, что первичное объективное отражение события остаётся в памяти электронных носителей в виде, который человек не способен напрямую воспринимать, в связи с чем информация приводится в понятный вид с помощью компьютерных устройств и программ, что, например, позволяет воспринимать такую информацию дистанционно, создавать её абсолютно идентичные копии [10, С. 168-170]. Однако в главах 24-27, 37 УПК РФ, которые посвящены следственным действиям и судебному следствию, не учитываются особенности взаимодействия с электронной информацией. В доктрине высказываются предложения о включении в УПК РФ группы

«электронных следственных действий». Например, М.С. Сергеев в своей диссертационной работе предложил закрепить в уголовно-процессуальном законе электронный осмотр, обыск, выемку и наблюдение, общей чертой которых будет направленность на обнаружение, восприятие и фиксацию электронной доказательственной информации [9, С. 17, 262].

Следует отметить, что досудебное доказывание имеет более поисковую природу, поэтому, будучи направленным на обнаружение и закрепление сведений в материалах уголовного дела, оно не гарантирует полноценной состязательности [11, С. 11-12]. Таким образом, полученные в ходе досудебного производства сведения становятся полноценными доказательствами в результате состязательного исследования в ходе судебного разбирательства, после чего они могут быть положены в основу приговора суда [4, С. 11-14]. В связи с чем в настоящей статье внимание будет сосредоточено на таком следственном действии, как осмотр, поскольку, в отличие от обыска и выемки, различные виды осмотра могут проводиться не только во время предварительного расследования, но и в ходе судебного разбирательства (284, 287 УПК РФ).

С.Б. Россинский определяет, что сущность осмотра заключается в непосредственном восприятии (изучении) фрагментов объективной реальности, а также их фиксации в протоколе с возможностью изъятия для приобщения к материалам уголовного дела [8, С. 180-181]. Автор указывает, что при наличии условий следователь должен стремиться к обеспечению возможности непосредственного исследования доказательства в судебном разбирательстве, так как протокол осмотра носит вторичный характер, поскольку, в отличие от прямого отражения следа, является повторным его отражением через сознание изготавливающего протокол лица [8, С. 183-184]. Таким образом, исследование электронных доказательств не обязательно должно ограничиваться лишь оглашением соответствующего протокола следственного действия, а может представлять непосредственное восприятие информации судом.

М.С. Сергеев подробно описывает порядок проведения электронного осмотра следователем, однако конструирует его исключительно как следственное действие для досудебных стадий (следователь является единственным участвующим субъектом доказывания, отсутствует вариант для главы 37 УПК РФ) [9, С. 313].

Следует согласиться с Р.И. Оконенко в том, что электронное доказательство не может быть исследовано путём только внешнего осмотра электронного носителя как предмета материального мира. Необходимо совершение действий в виртуальной среде, которые направлены на установление содержания такого носителя, например, открытие файлов, папок с файлами, изучение их свойств, в том числе с применением подходящего программного обеспечения [6, С. 8-9]. Аналогичную мысль высказал В.В. Момотов, поскольку в судебном разбирательстве электронные доказательства должны быть визуализированы, исследованы надлежащим образом, в противном случае невозможно установить и учесть их содержание [5, С. 5].

К.Ю. Яковлева также предлагает закрепить понятие дистанционного осмотра электронной информации, понимая под этим выявление, изъятие и фиксацию информации, к которой предоставляется доступ неограниченного круга лиц [13, С. 43-44]. Заслуживает поддержки её вывод о том, что электронная информация по возможности должна быть сохранена в первоначальном (электронном) виде, поскольку таким образом остаются зафиксированы различные метаданные, которые могут быть утеряны при

переносе в формат бумажного документа. Для подтверждения достоверности электронной информации ей выдвинуто предложение о фиксации в протоколах следственных и иных процессуальных действий контрольной суммы электронной информации [14, С. 43]. Контрольная сумма файла представляет собой строку символов, получаемую в результате работы математического алгоритма, который не затрагивает содержимое исходной информации. Контрольные суммы совпадают при тождественности самих электронных документов и позволяют установить аутентичность электронного документа подобно штампу или печати на бумажном документе [18, С. 16]. Таким образом можно установить идентичность копии и оригинала электронной информации, а также идентичность одного и того же материала самому себе в разные периоды времени, например в момент осмотра следователем и судом. Достаточно сравнить контрольную сумму, зафиксированную в протоколе на момент осмотра доказательства следователем, и вновь установленную во время осмотра в суде. Если они совпадают, то сведения остались неизменными, что позволяет продемонстрировать, что достоверность электронного доказательства не была нарушена с момента его собирания до момента исследования в суде.

В то же время представляется ошибочным утверждение о том, что возможен осмотр исключительно общедоступных сведений. Субъекты доказывания могут проводить осмотр информации, которая, хотя и не находится в свободном доступе для неограниченного круга лиц, а, например, защищена паролем, но добровольно представляется владельцем для включения в доказательственную базу. В таком случае отсутствует поиск и принудительное изъятие сведений без согласия их обладателя, которое характерно для обыска и выемки.

В отношении электронных следственных действий критерием разграничения является осведомленность владельца информации о проведении в отношении информации следственных действий и наличие его добровольного согласия, а также тип осматриваемого устройства [12, С. 103]. Таким образом, прослеживается понятное разграничение. Осмотр электронных доказательств — это наблюдение (исследование) и фиксация доступной субъекту доказывания электронной информации с сохранением её целостности, в то время как обыск или выемка предполагают отыскание и изъятие электронных носителей информации или самой информации вопреки воле её владельца. Представляется, что осмотр может быть следующим шагом после изъятия, поскольку следователю необходимо ознакомиться с полученной информацией, выяснить её содержание и сделать вывод о её соответствии признакам, которые закон предъявляет к доказательствам, по возможности зафиксировать её контрольную сумму.

Помимо доктринальных разработок отечественных учёных, несомненный интерес представляет и опыт зарубежных стран, которые включили в законодательство нормы, регламентирующие отдельные особенности осмотра электронных доказательств.

Так, согласно ч. 3 ст. 110 УПК ФРГ, допускается осмотр электронных носителей лица, подвергшегося обыску [1]. Такой осмотр может распространяться на находящиеся на удалённом расстоянии электронные носители, доступные с первоначального устройства, когда существует риск, что в противном случае искомые данные будут утрачены. В ходе судебного следствия каких-либо специальных правил по осмотру электронных доказательств прямо не предусмотрено, однако следует отметить ч. 5 ст. 244 УПК ФРГ, закрепляющую общее правило о том, что ходатайство о производстве осмотра может быть отклонено, если по дискреционному усмотрению суда такой осмотр не является необходимым для установления истины. Такой подход позволяет обезопасить процесс от

чрезмерного потока сомнительной электронной информации, достоверность которой суд подтвердить не может, а доказательственная ценность которой мала либо неочевидна.

В УПК Французской Республики существует статья 57-1, регулирующая осмотр компьютерных систем [2]. Согласно ей, проводящие обыск лица вправе получить доступ к значимой для расследования информации в компьютерной системе в обыскиваемом помещении либо находящейся на расстоянии компьютерной системе, доступ к которой возможен при использовании первоначальной. Правоохранители имеют право в предусмотренной законом форме потребовать от любого лица, которое может быть осведомлено о мерах, применённых для защиты данных, доступ к которым осуществляется в рамках обыска, передачи информации, обеспечивающей доступ к указанным данным. Стоит отметить, что упомянутый осмотр компьютерных систем скорее составляет элемент обыска, что в целом характерно для зарубежных стран в случаях, когда осмотр носит принудительный характер [1].

Особый интерес представляет УПК Республики Беларусь, где получила закрепление статья 204.1 «Осмотр компьютерной информации» [3]. Данная норма предоставляет ряд дополнительных гарантий владельцам электронных носителей. Так, осмотр информации, доступ к которой осуществляется посредством аутентификации пользователя (например, вводом пароля или сканированием отпечатка пальца), либо информации, составляющей личную или иную охраняемую законом тайну, либо иным образом ограниченной в распространении, возможен только с согласия владельца такой информации либо с санкции прокурора (за исключением случаев, не терпящих отлагательств). В случае, если компьютерная информация или аутентификационные данные были ранее получены в ходе следственного действия, санкционированного прокурором, повторно получать разрешение на осмотр такой информации не требуется. Подобный подход представляется достаточно гибким и, с одной стороны, гарантирует владельцам информации защиту от необоснованного доступа к ней, но и допускает возможность лиц, ведущих расследование, провести с одобрения прокурора осмотр информации, имеющей важное значение для расследования. Для обеспечения допустимости полученных доказательств ведётся протокол с указанием, какое оборудование использовалось в ходе осмотра, как осуществлялся доступ к информации, какие действия с ней проводились и какие результаты были получены.

Приведённые примеры показывают, что отечественные исследователи и зарубежные законодатели, как правило, не выделяют особенностей осмотра электронных доказательств во время судебного разбирательства. Это характерно и для российского уголовного процесса. На сегодняшний день в судебном разбирательстве осмотр электронных носителей проводится по правилам ст. 284 УПК РФ, которая регулирует осмотр вещественных доказательств. Использование данной статьи может вызывать затруднения при переходе к облачному способу хранения электронных доказательств, когда исследуемые данные сохранены в виртуальном формате, например системе электронного уголовного дела, как это имеет место в Республике Казахстан [2, С. 90]. В таком случае отсутствует явно обособленный, приобщённый к материалам уголовного дела предмет, сохранивший следы преступления. Также в судебной практике нередко встречается ситуация, когда сторона защиты в апелляционной жалобе указывает, что суд положил в основу приговора неисследованное электронное доказательство. Как правило, суды вышестоящей инстанции отмечают, что процессуальные нормы не нарушены. Например, в апелляционном определении судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 28.02.2025 по делу № 22-576/2025

установлено, что все протоколы обнаружения и изъятия мобильных и компьютерных устройств, электронных носителей информации исследованы судом первой инстанции, стороной защиты ходатайства о непосредственном осмотре в порядке 284 УПК РФ заявлено не было. Таким образом, суд апелляционной инстанции пришёл к выводу, что порядок исследования доказательств не был нарушен.

Ещё одной проблемой являются пределы осмотра электронного носителя, на котором хранится доказательство. Как верно отмечает С.Г. Коновалов, признание единичного электронного документа самостоятельным доказательством позволяет избежать ситуации, когда по логике закона суд обязан ознакомиться с содержимым электронного носителя как с обычным вещественным доказательством, то есть исследовать его полным и всесторонним образом, что практически невозможно, а логически нецелесообразно, когда, например, сторона представляет для исследования свой мобильный телефон, содержащий сотни неотносимых к делу файлов [3]. Подобная мысль подтверждается судебной практикой, например, Седьмой кассационный суд общей юрисдикции в постановлении от 23 ноября 2023 г. по делу № 7У-9741/2023[77-4574/2023] указал, что электронный носитель, в частности диск, может не иметь самостоятельного доказательственного значения, поскольку в доказательственную базу входят именно конкретные сведения, записанные на этот диск. Ключевое значение имеет то, чтобы эти сведения получались и исследовались в соответствии с законом.

Согласно ст. 240 УПК РФ, в обоснование приговора могут быть положены только непосредственно исследованные доказательства. В указанной статье перечислены способы исследования доказательств, а именно: заслушивание показаний или заключений, оглашение протоколов и иных документов, осмотр вещественных доказательств, кроме того, перечень открыт и предполагает, что могут быть проведены судебные действия по исследованию доказательств. Заслушивание предлагает выступление живого человека, который в устной форме сообщает перед судом и сторонами какую-либо информацию. Оглашение уместно для текстовых данных, в том числе представленных в виде электронного документа, однако при необходимости восприятия визуального, динамического, смешанного контента (изображение, аудио-, видеозапись, метаданные файла) следует проводить осмотр электронного доказательства с фиксацией используемых устройств, последовательности действий, свойств и содержания исследуемой информации.

Во время судебного разбирательства могут быть осмотрены несколько видов электронной информации, имеющей доказательственное значение, природа которых различается.

Первый вариант — это сведения, которые были ранее собраны и приобщены в качестве доказательств на досудебных стадиях. Они получили предварительное процессуальное оформление, их допустимость подтверждается тем, что они собраны (сформированы) надлежащими субъектами в ходе процедур, предусмотренных уголовно-процессуальным законом. На момент судебного разбирательства такие сведения уже должны были пройти проверку подлинности, если она была необходима, например, путём проведения экспертизы. Как правило, в материалах уголовного дела также имеются протоколы следственных и иных процессуальных действий, отражающие порядок собирания и приобщения электронных доказательств. Данные документы имеет смысл огласить перед непосредственным исследованием электронного носителя и содержащейся на нём информации, поскольку таким образом суд может установить основания и законность появления конкретного электронного доказательства в материалах уголовного дела, обстоятельства его хранения, характеристики электронной информации (например,

сравнить контрольную сумму, если она фиксировалась) и другие имеющие значение сведения.

Как отмечалось ранее, в судебной практике признаётся допустимым оглашение протокола осмотра электронной информации, который проводился следователем на досудебных стадиях уголовного процесса. Вместе с тем у некоторых участников судопроизводства возникает недопонимание, которое приводит к обжалованию приговора по причине его обоснования неисследованными доказательствами. Чтобы избежать подобного диссонанса, суд имеет возможность после оглашения протокола следственного действия выяснить мнение сторон о необходимости непосредственного осмотра электронной информации, которая была описана в протоколе следственного действия.

Следующим вариантом является информация на электронных носителях, которые стороны принесли для осмотра и приобщения в качестве доказательства в ходе судебного разбирательства. Получение новых доказательств в судебном разбирательстве допускается в силу разъяснения Конституционного суда РФ, согласно которому закон не допускает произвольного отказа в приобщении и исследовании судом доказательств, за исключением ситуаций, когда такие сведения не относятся к рассматриваемому делу, с их помощью невозможно установить обстоятельства, подлежащие доказыванию, сведения получены с нарушением закона, либо устанавливаемое при помощи этих сведений обстоятельство уже нашло подтверждение или было опровергнуто при помощи достаточной совокупности доказательств[4]. Таким образом, следует выяснить, законно ли собрана данная информация, не нарушались ли при её получении права граждан и организаций, имеет ли она отношение к рассматриваемому делу, почему она не была приобщена ранее, на этапе предварительного расследования (соответствие ст. 75 УПК РФ). Суд может как принять такие доказательства без дополнительной проверки, так и направить электронный носитель для проведения экспертизы его подлинности.

Третья ситуация возникает, когда исследуется электронная информация, находящаяся в информационно-телекоммуникационных сетях, например сети «Интернет». Очевидно, что в ходе судебного следствия невозможен поиск новой, ранее неизвестной для сторон информации в глобальной сети, поскольку это превратило бы суд в полицейский субъект, самостоятельно занимающийся поиском доказательств, что противоречило бы принципу состязательности сторон (ст. 15 УПК РФ).

В то же время, существуют примеры обращения судов к глобальным сетям. Передовым в вопросе осмотра сайтов является арбитражный процесс. Согласно разъяснению Пленума Верховного суда РФ, суд при подготовке дела к слушанию наделён правом получать необходимые сведения из открытых источников, в частности государственных информационных систем, в том числе посредством сети «Интернет». Если обратиться к п. 3 ст. 135 АПК РФ, то становится понятно, что речь идёт именно о содействии сторонам в получении необходимых доказательств либо получении доказательств по инициативе суда.

В иностранных публикациях относительно осмотра сайтов встречаются споры о том, возможно ли применение judicial notice, то есть правила о признании общеизвестных фактов без их дополнительной проверки. Суть подобного правила заключается в том, что суд может осмотреть сайт и принять во внимание размещённую на нём информацию без дополнительной проверки, не требуя, например, нотариального удостоверения и не

назначая экспертизу [15, С. 194]. Как правило, без дополнительной проверки информация берётся только с государственных официальных сайтов (сайты органов государственной власти, государственные реестры, сайты с официальной статистикой и им подобные). В то же время иные сайты требуют проверки размещённой на них информации, поскольку она может оказаться недостоверной или изменённой [15, С. 194-195]. Авторы подчёркивают, что сведения из открытых интернет-источников могут обладать существенной ценностью для доказывания [С. 1254]. Однако традиционные правила о допустимости доказательств недостаточно приспособлены к специфике цифрового контента, что требует критической оценки и осторожности при их использовании [16, С. 1253]. Кроме того, состязательная природа уголовного процесса подразумевает ограниченную активность суда, поэтому инициировать такой осмотр должно волеизъявление участвующей в процессе стороны.

Таким образом, в случае наделения суда правом по ходатайству стороны проводить осмотр заранее известной страницы и/или сайта в сети «Интернет», следует предусмотреть такие процессуальные рамки, которые позволили бы суду избежать включения в доказательственную базу ненадёжной информации. Например, установление перечня сайтов государственных органов и организаций, где публикуется официально подтверждённая информация, которую суд может принять без дополнительной проверки. Кроме того, существует возможность запроса дополнительных сведений у владельца сайта, провайдера, государственных органов и назначения экспертизы подлинности размещённой в сети информации. Кроме того, как ранее отмечалось, суд имеет право отказать в удовлетворении ходатайства, если становится понятно, что подлежащий установлению при помощи осмотра сайта факт уже был подтверждён или опровергнут достаточным количеством доказательств, либо осматриваемая информация не относится к слушаемому делу или не может подтвердить или опровергнуть искомые факты.

Ход и результаты осмотра электронных доказательств, использованные технические и программные средства должны быть отражены в протоколе судебного разбирательства, составлять отдельный протокол или акт не требуется [7, С. 9]. Поскольку цифровые ресурсы могут быть изменены, отредактированы, имеет смысл сохранение электронной информации в более стабильном виде и её приобщение к материалам дела, например, в виде распечатки или электронной копии [7, С. 10, 13].

В качестве итогов исследования могут быть сформулированы следующие выводы.

1. В научной литературе, а также законодательстве ряда зарубежных стран, осмотр электронных доказательств (его аналоги) чаще всего рассматривается в качестве следственного действия, проводимого для собирания доказательств на досудебном этапе. Осмотр электронных доказательств как судебное действие анализируется достаточно редко.

2. Осмотр электронной доказательственной информации представляет собой следственное действие, направленное на непосредственное восприятие и фиксацию следователем (дознавателем) или судом электронной информации. Допускается использование необходимых для исследования электронной информации устройств и компьютерных программ, взаимодействие с информацией, которое не нарушает её целостность (например, ввод пароля для просмотра защищённых им документов, увеличение (приближение) отдельных элементов цифрового изображения и др.). В досудебных стадиях нередко происходит фактически обыск (выемка) электронных

ресурсов, а затем осмотр информации в качестве самостоятельного следственного действия. В судебном разбирательстве проведение обыска или выемки не допускается, в связи с чем осмотр остаётся наиболее подходящим следственным действием для исследования электронных доказательств.

3. Могут быть выделены три возможные ситуации, в ходе которых в судебном разбирательстве исследуется электронная информация:

а) осмотр электронных доказательств, собранных в ходе предварительного расследования;

б) осмотр и приобщение в качестве доказательства электронной информации на электронном носителе, который предоставлен стороной непосредственно в судебное разбирательство по ходатайству этой стороны;

в) осмотр находящихся в открытом доступе страниц и/или сайтов в сети «Интернет» и приобщение электронной информации в качестве доказательства по ходатайству стороны.

На основании проведённого исследования автором сформулировано предложение о дополнении УПК РФ статьёй 284.1 «Осмотр и приобщение электронных доказательств» следующего содержания:

1. Осмотр электронных доказательств осуществляется по ходатайству стороны в любой момент судебного следствия в зале заседания или в ином специально оборудованном помещении. При необходимости могут быть использованы технические и программные средства, приглашён специалист.

2 . Допускается приобщение электронных доказательств по ходатайству стороны судебного разбирательства путём предоставления суду электронного носителя либо копирования информации на иной электронный носитель, который предоставляется суду.

3. Осмотр открытых источников в информационно-коммуникационных сетях, в том числе сети «Интернет», осуществляется судом по ходатайству стороны при наличии технической возможности. Ходатайство стороны об осмотре сайта или страницы в сети «Интернет» может быть отклонено, если подлежащий установлению факт подтверждается ранее исследованной достаточной совокупностью доказательств либо подлежащая исследованию информация не отвечает требованиям, предъявляемым настоящим кодексом к доказательствам.

4. Ход осмотра фиксируется в протоколе судебного разбирательства, делаются отметки об использованных технических устройствах и программном обеспечении. По определению суда к материалам уголовного дела может быть приобщена копия осмотренных сведений.

Подобный подход позволит расширить использование в доказывании по уголовному делу электронных доказательств, обеспечить их непосредственное исследование, сохраняя определённые рамки, позволяющие суду не допустить использование в доказывании произвольной информации, которую стороны желают ввести в процесс.

[1] German Code of Criminal Procedure // URL: https://www.gesetze-im-internet.de/englisch_stpo/index.html#gl_p0962

[2] Code de procédure pénale // URL:

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047053305

[3] Уголовно-процессуальный кодекс Республики Беларусь // URL: https://pravo.by/document/?guid=3871&p0=HK9900295

[4] Определение Конституционного Суда РФ от 04.04.2006 № 100-О // URL: https://www.consultant.ru/document/cons_doc_LAW_60927/

Библиография

1. Зуев С.В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58-60. EDN: UNYMRO.
2. Зуев С. В., Моругина Н. А. Электронное уголовное дело: теоретическая модель // Вестник Казанского юридического института МВД России. 2024. № 3 (57). С. 83-94. DOI: 10.37973/VESTNIKKUI-2024-57-9. EDN: CQSDYT.
3. Коновалов С.Г. Использование в уголовном процессе цифровых данных, хранящихся в телефоне: назревшие вопросы и пути их решения // Закон. 2021. № 11. С. 128-138. DOI: 10.37239/0869–4400-2021-16-11-128-138. EDN: NCNSAA.
4. Кухта А.А. Доказывание истины в уголовном процессе: автореф. дис. … док. юрид. наук: 12.00.09. Нижний Новгород, 2012. 61 с.
5. Момотов В.В. Электронное правосудие в Российской Федерации: миф или реальность? // Российская юстиция. 2021. № 7. С. 2-9.
6. Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дис. … кан. юрид. наук: 12.00.09. М., 2016. 158 с. EDN: VMNEAE.
7. Плотников А., Харитонюк К. Электронное судопроизводство и рассмотрение электронных доказательств при рассмотрении дел экономическими судами // Судебный вестник Плюс: экономическое правосудие. 2021. № 8. С. 4-13.
8. Россинский С.Б. Следственные действия: монография. М. Норма, 2018. 240 с. EDN: ZSYGNX.
9. Сергеев М.С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: дис. … канд. юрид. наук: 12.00.09. Казань, 2018. 322 с. EDN: RWUZOU.
10. Смушкин А.Б. "Концепция электронных" следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. № 3. С. 165-172. DOI: 10.24412/2587–9820-2021-3-165-172. EDN: MPMSKP.
11. Хмельницкая Т.В. Проблемы формирования доказательств в ходе досудебного производства по уголовному делу: дис. … канд. юрид. наук: 12.00.09. Нижний Новгород, 2016. 213 с. EDN: WFMQYF.
12. Черкасов В.С. Проблема разграничения следственных действий: осмотр и обыск при получении компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 99-103. EDN: YWUJVG.
13. Яковлева К.Ю. Собирание доказательств, содержащих электронную информацию, в уголовном процессе (на примере осмотра) // Уголовное судопроизводство. 2023. № 1. С. 40-44. DOI: 10.18572/2072–4411-2023-1-40-44. EDN: IGXXTJ.
14. Яковлева К.Ю. Контрольная сумма как элемент достоверности доказательства, содержащего электронную информацию, в уголовном процессе // Российский следователь. 2024. № 2. С. 39-43. DOI: 10.18572/1812–3783-2024-2-39-43. EDN: QTOFGL.
15. Jones S. Trial by Google Maps? The Dangers of Admitting Privatized GIS Technology by

Judicial Notice // California Western Law Review. 2023. Vol. 60, Iss. 1, Article 7. P. 185-219.
16. Koenig A., Freeman L. Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation // Hastings Law Journal. 2022. Vol. 73, Iss. 5. P. 1233–1254.
17. Mason, S., & Seng, D. (Eds.). Electronic Evidence and Electronic Signatures (5th ed.). Institute of Advanced Legal Studies, University of London Press. 2021. 540 p.
18. Novak M. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration // Journal of Digital Forensics, Security and Law. 2020. Vol. 14, Article 3. '''

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье является, как это следует из ее наименования, осмотр электронных доказательств в уголовном процессе. Автор сосредоточил внимание на анализе судебного аспекта проблемы. Заявленные границы исследования соблюдены ученым.
Методология исследования в тексте статьи не раскрывается.
Актуальность избранной автором темы исследования несомненна и обосновывается им следующим образом: "В современном уголовном судопроизводстве часто возникает необходимость обращения к различной электронной информации, имеющей доказательственное значение. Примером являются аудио- или видеозаписи, сведения с сайтов и страниц в сети «Интернет», переписка в социальных сетях, мессенджерах, лог-файлы, метаданные и иные данные, при помощи которых устанавливаются обстоятельства, подлежащие доказыванию [17, С. 23-33]" и др. Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.
Научная новизна работы проявляется в ряде заключений автора: "В то же время представляется ошибочным утверждение о том, что возможен осмотр исключительно общедоступных сведений. Субъекты доказывания могут проводить осмотр информации, которая, хотя и не находится в свободном доступе для неограниченного круга лиц, а, например, защищена паролем, но добровольно представляется владельцем для включения в доказательственную базу. В таком случае отсутствует поиск и принудительное изъятие сведений без согласия их обладателя, которое характерно для обыска и выемки"; "Приведённые примеры показывают, что отечественные исследователи и зарубежные законодатели, как правило, не выделяют особенностей осмотра электронных доказательств во время судебного разбирательства. Это характерно и для российского уголовного процесса. На сегодняшний день в судебном разбирательстве осмотр электронных носителей проводится по правилам ст. 284 УПК РФ, которая регулирует осмотр вещественных доказательств. Использование данной статьи может вызывать затруднения при переходе к облачному способу хранения электронных доказательств, когда исследуемые данные сохранены в виртуальном формате, например системе электронного уголовного дела, как это имеет место в Республике Казахстан [2, С. 90]. В таком случае отсутствует явно обособленный, приобщённый к материалам уголовного дела предмет, сохранивший следы преступления. Также в судебной практике нередко встречается ситуация, когда сторона защиты в апелляционной жалобе указывает, что суд положил в основу приговора неисследованное электронное

доказательство. Как правило, суды вышестоящей инстанции отмечают, что процессуальные нормы не нарушены"; "Как отмечалось ранее, в судебной практике признаётся допустимым оглашение протокола осмотра электронной информации, который проводился следователем на досудебных стадиях уголовного процесса. Вместе с тем у некоторых участников судопроизводства возникает недопонимание, которое приводит к обжалованию приговора по причине его обоснования неисследованными доказательствами. Чтобы избежать подобного диссонанса, суд имеет возможность после оглашения протокола следственного действия выяснить мнение сторон о необходимости непосредственного осмотра электронной информации, которая была описана в протоколе следственного действия"; "Таким образом, в случае наделения суда правом по ходатайству стороны проводить осмотр заранее известной страницы и/или сайта в сети «Интернет», следует предусмотреть такие процессуальные рамки, которые позволили бы суду избежать включения в доказательственную базу ненадёжной информации. Например, установление перечня сайтов государственных органов и организаций, где публикуется официально подтверждённая информация, которую суд может принять без дополнительной проверки. Кроме того, существует возможность запроса дополнительных сведений у владельца сайта, провайдера, государственных органов и назначения экспертизы подлинности размещённой в сети информации" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан автором в полной мере.

Структура работы логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор анализирует судебный аспект проблемы осмотра электронных доказательств в уголовном процессе и предлагает пути ее решения. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание работы соответствует ее наименованию и не вызывает особых нареканий.

Библиография исследования представлена 18 источниками (диссертационными работами, монографией, научными статьями), в том числе на английском языке. С формальной и фактической точек зрения этого достаточно. Автору удалось раскрыть тему исследования с необходимой полнотой и глубиной.

Апелляция к оппонентам имеется, как общая, так и частная (М. С. Сергеев), и вполне достаточна. Научная дискуссия ведется автором корректно. Положения работы обоснованы в должной степени и проиллюстрированы примерами.

Выводы по результатам проведенного исследования имеются ("1. В научной литературе, а также законодательстве ряда зарубежных стран, осмотр электронных доказательств (его аналоги) чаще всего рассматривается в качестве следственного действия, проводимого для собирания доказательств на досудебном этапе. Осмотр электронных доказательств как судебное действие анализируется достаточно редко. 2. Осмотр электронной доказательственной информации представляет собой следственное действие, направленное на непосредственное восприятие и фиксацию следователем (дознавателем) или судом электронной информации. Допускается использование необходимых для исследования электронной информации устройств и компьютерных программ, взаимодействие с информацией, которое не нарушает её целостность (например, ввод пароля для просмотра защищённых им документов, увеличение (приближение) отдельных элементов цифрового изображения и др.). В досудебных стадиях нередко происходит фактически обыск (выемка) электронных ресурсов, а затем осмотр информации в качестве самостоятельного следственного действия. В судебном разбирательстве проведение обыска или выемки не допускается, в связи с чем осмотр остаётся наиболее подходящим следственным действием для исследования электронных

доказательств. 3. Могут быть выделены три возможные ситуации, в ходе которых в судебном разбирательстве исследуется электронная информация: а) осмотр электронных доказательств, собранных в ходе предварительного расследования; б) осмотр и приобщение в качестве доказательства электронной информации на электронном носителе, который предоставлен стороной непосредственно в судебное разбирательство по ходатайству этой стороны; в) осмотр находящихся в открытом доступе страниц и/или сайтов в сети «Интернет» и приобщение электронной информации в качестве доказательства по ходатайству стороны" и др.), они четкие, конкретные, обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного процесса при условии ее небольшой доработки: раскрытии методологии исследования и дополнительном обосновании актуальности его темы (в рамках сделанного замечания).